



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,884	03/08/2002	Jean-Sebastien Coron	032326-161	5848
21839	7590	02/08/2007	EXAMINER	
BUCHANAN, INGERSOLL & ROONEY PC			HENNING, MATTHEW T	
POST OFFICE BOX 1404			ART UNIT	PAPER NUMBER
ALEXANDRIA, VA 22313-1404			2131	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		02/08/2007	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	09/913,884	CORON ET AL.	
	Examiner Matthew T. Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 15 November 2006.  
 2a) This action is FINAL.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 24-37 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 24-37 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 29 March 2006 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____	5) <input type="checkbox"/> Notice of Informal Patent Application
	6) <input type="checkbox"/> Other: _____

Art Unit: 2131

1                   This action is in response to the communication filed on 11/15/2006.

2                   **DETAILED ACTION**

3                   *Response to Arguments*

4                   Applicant's arguments with respect to claims 24-37 have been considered but are moot in  
5                   view of the new ground(s) of rejection.

6                   All rejections and objections not set forth below have been withdrawn.

7                   Claims 1-23 have been cancelled and claims 24-37 have been examined.

8                   *Priority*

9                   Applicant has relied upon the foreign priority papers to overcome the previous prior art  
10                  rejection by making of record a translation of said papers in accordance with 37 CFR 1.55. See  
11                  MPEP § 201.15. As such, the previous rejection in view of Ohki et al. has been withdrawn.

13                   *Claim Rejections - 35 USC § 103*

14                  The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all  
15                  obviousness rejections set forth in this Office action:

16                  (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in  
17                  section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are  
18                  such that the subject matter as a whole would have been obvious at the time the invention was made to a person  
19                  having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the  
20                  manner in which the invention was made.

21                  Claims 24-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et  
22                  al. (US Patent Number 6,278,783) hereinafter referred to as Kocher1, and further in view of  
23                  Kocher et al. (US Patent Number 6,327,661) hereinafter referred to as Kocher2.

25                  Regarding claim 24, Kocher1 disclosed a countermeasure method in an electronic  
26                  component that implements the DES cryptographic algorithm in which multiple rounds of

Art Unit: 2131

1 calculation are performed on input data (See Kocher1 Abstract), wherein each round of  
2 calculation includes at least the following operations: a first permutation of data (See Kocher1  
3 Col. 10 Lines 55-60); manipulation of the permuted data by a secret key (See Kocher1 Col. 10  
4 Line 61 – Col. 11 Line 5); a table look-up operation based on the manipulated data (See Kocher1  
5 Col. 11 Lines 6-7); and a second permutation of data (See Kocher1 Col. 11 Lines 7-11), but  
6 Kocher1 failed to disclose wherein, for a plurality of successive rounds of said algorithm, at least  
7 one of said first and second permutations of data comprises the following steps: selecting a first  
8 random value having the same size as the data being permuted, performing an exclusive-or  
9 operation between the data being permuted and the first random value to generate a second  
10 random value, executing said permutation operation on each of the first and second random  
11 values, to generate respective first and second random results, and performing an exclusive-or  
12 operation between said first and second random results to produce a final permuted result.

13 Kocher2 teaches that in order to protect against external monitoring attacks, processes,  
14 including DES permutations, should be performed using a leak-minimized permutation operation  
15 (See Kocher2 Col. 10 Line 50 – Col. 13 Line 19). Kocher further describes that the permutation  
16 operations should be altered by selecting a first random value having the same size as the data  
17 being permuted, performing an exclusive-or operation between the data being permuted and the  
18 first random value to generate a second random value, executing said permutation operation on  
19 each of the first and second random values, to generate respective first and second random  
20 results, and performing an exclusive-or operation between said first and second random results to  
21 produce a final permuted result (See Kocher Col. 12 Lines 20-60).

Art Unit: 2131

1        It would have been obvious to the ordinary person skilled in the art at the time of  
2 invention to employ the teachings of Kocher2 in the DES system of Kocher1 by performing the  
3 permutation processing according to the leak-minimized permutation operation. This would  
4 have been obvious because the ordinary person skilled in the art would have been motivated to  
5 protect the permutation processing from external monitoring attacks.

6        Regarding claim 31, Kocher1 disclosed an electronic component that implements the  
7 DES cryptographic algorithm in which multiple rounds of calculation are performed on input  
8 data, said electronic component including a microprocessor that executes the following  
9 operations during each round of calculation (See Kocher1 Abstract): a first permutation of data  
10 (See Kocher1 Col. 10 Lines 55-60); manipulation of the permuted data by a secret key (See  
11 Kocher1 Col. 10 Line 61 – Col. 11 Line 5); a table look-up operation based on the manipulated  
12 data (See Kocher1 Col. 11 Lines 6-7); and a second permutation of data (See Kocher1 Col. 11  
13 Lines 7-11), but Kocher1 failed to disclose wherein, for a plurality of successive rounds of said  
14 algorithm, at least one of said first and second permutations of data comprises the following  
15 steps: selecting a first random value having the same size as the data being permuted, performing  
16 an exclusive-or operation between the data being permuted and the first random value to  
17 generate a second random value, executing said permutation operation on each of the first and  
18 second random values, to generate respective first and second random results, and performing an  
19 exclusive-or operation between said first and second random results to produce a final permuted  
20 result.

21        Kocher2 teaches that in order to protect against external monitoring attacks, processes,  
22 including DES permutations, should be performed using a leak-minimized permutation operation

Art Unit: 2131

1 (See Kocher2 Col. 10 Line 50 – Col. 13 Line 19). Kocher further describes that the permutation  
2 operations should be altered by selecting a first random value having the same size as the data  
3 being permuted, performing an exclusive-or operation between the data being permuted and the  
4 first random value to generate a second random value, executing said permutation operation on  
5 each of the first and second random values, to generate respective first and second random  
6 results, and performing an exclusive-or operation between said first and second random results to  
7 produce a final permuted result (See Kocher Col. 12 Lines 20-60).

8 It would have been obvious to the ordinary person skilled in the art at the time of  
9 invention to employ the teachings of Kocher2 in the DES system of Kocher1 by performing the  
10 permutation processing according to the leak-minimized permutation operation. This would  
11 have been obvious because the ordinary person skilled in the art would have been motivated to  
12 protect the permutation processing from external monitoring attacks.

13 Regarding claims 25 and 32, Kocher1 and Kocher2 disclosed performing both of said  
14 first and second permutation operations in each of said plurality of successive rounds (See the  
15 rejection of claims 24 and 31 above).

16 Regarding claims 26 and 33, Kocher1 and Kocher2 disclosed that the first and second  
17 permutation operations utilize different respective first random values (See Kocher2 Col. 12  
18 Lines 45-47).

19 Regarding claims 27 and 34, Kocher1 and Kocher2 disclosed that said plurality of  
20 successive rounds comprise a first set of successive rounds consisting of the first three rounds of  
21 said algorithm, and a second set of successive rounds consisting of the last three rounds of said  
22 algorithm (See the rejection of claims 24 and 31 above as well as Kocher1 Fig. 1).

Art Unit: 2131

1       Regarding claims 28 and 35, Kocher1 and Kocher2 disclosed that the manipulation  
2 operation performed during said plurality of successive rounds comprises the following steps:  
3 performing an exclusive-or operation between said secret key and a third random value having  
4 the same size as said key, to generate a fourth random value; performing bit-by-bit operations on  
5 each of said third and fourth random values to produce a pair of intermediate keys; manipulating  
6 the result of said first permutation operation with one of said intermediate keys to produce an  
7 intermediate result, and manipulating said intermediate result with the other of said intermediate  
8 keys to produce an output data item (See Kocher1 Col. 10 Lines 16-24 and the rejections of  
9 claims 24 and 31 above).

10       Regarding claims 29 and 36, Kocher1 and Kocher2 disclosed that said manipulating steps  
11 comprise exclusive-or operations (See Kocher2 Col. 12 Lines 45-50).

12       Regarding claims 30 and 37, Kocher1 and Kocher2 disclosed that said bit-by-bit  
13 operations comprise a key permutation operation, a shift operation and a compression  
14 permutation operation (See Kocher1 Col. 10 Lines 16-24).

### *Conclusion*

16       Claims 1-23 have been cancelled and claims 24-37 have been rejected.

17       A shortened statutory period for reply to this final action is set to expire THREE  
18 MONTHS from the mailing date of this action. In the event a first reply is filed within TWO  
19 MONTHS of the mailing date of this final action and the advisory action is not mailed until after  
20 the end of the THREE-MONTH shortened statutory period, then the shortened statutory period  
21 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37  
22 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131

1 however, will the statutory period for reply expire later than SIX MONTHS from the date of this  
2 final action.

3 Any inquiry concerning this communication or earlier communications from the  
4 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.

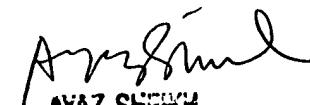
5 The examiner can normally be reached on M-F 8-4.

6 If attempts to reach the examiner by telephone are unsuccessful, the examiner's  
7 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the  
8 organization where this application or proceeding is assigned is 571-273-8300.

9 Information regarding the status of an application may be obtained from the Patent  
10 Application Information Retrieval (PAIR) system. Status information for published applications  
11 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished  
12 applications is available through Private PAIR only. For more information about the PAIR  
13 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR  
14 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would  
15 like assistance from a USPTO Customer Service Representative or access to the automated  
16 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

17  
18  
19  
20  
21

22   
Matthew Henning  
23 Assistant Examiner  
24 Art Unit 2131  
25 2/2/2007

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

26